Mostafa Soliman / Int.J.Cryp.Curr.Res. 3(1) (2023) 74-77
https://doi.org/10.51483/IJCCR.3.1.2023.74-77
ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Layers of the Internet: The Challenge of the Dark Web and the Need for an International Legal Framework

Mostafa Soliman[1]*

[1]Independent Researcher, USA. E-mail: mostafasoliman.am@gmail.com

Article Info

Volume 3, Issue 1, June 2023
Received : 21 January 2023
Accepted : 14 May 2023
Published : 05 June 2023
doi: 10.51483/IJCCR.3.1.2023.74-77

Abstract

The Dark Web and Dark Net, or Darknet, have become buzzwords in recent years, particularly around cybercrime and illicit activities. They refer to a hidden part of the internet that is not easily accessible by traditional search engines or browsers. The Dark Web operates through encrypted networks, such as Tor, which allow users to browse the internet anonymously. The Dark Web has been associated with illicit activities such as the sale of illegal drugs, firearms, and even human trafficking. These activities are facilitated through the use of cryptocurrency transactions, making it difficult for law enforcement agencies to track the movements of money and identify the individuals involved in such transactions. Activities on the Dark Web however are not all illegal. There are legitimate uses such as political dissent and whistleblowing. Many journalists and activists use the Dark Web to communicate and share information securely. The Dark Web also has the potential to be a tool for good, such as providing a safe space for marginalized communities to connect and organize, away from the scrutiny of those who seek to oppress them. This paper discusses the legal framework for the Dark Web activities. The Dark Web still remains a source of illicit activity, and law enforcement agencies around the world are working to dismantle criminal networks and apprehend those responsible for facilitating illegal activities on the Dark Web. As technology continues to evolve, it is likely that the Dark Web will continue to be a challenge for law enforcement and a platform for criminal activity, both nationally and internationally.

Keywords: *Dark Web, Darknet, Encrypted networks, Legal framework*

© 2023 Mostafa Soliman. This is an open access article under the CCBY license (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

1. Introduction

The terms Dark Web and Dark Net, or Darknet, are often used interchangeably, but they technically refer to different things.[1] The Internet is comprised of three main parts: Surface Net, Deep Web, and Dark Web.[2] The Surface Net consists of websites that are searchable and accessible through common search engines like Google and Bing.[3] The Deep Web, on the other hand, includes the parts of the Internet that cannot be accessed

* *Corresponding author: Mostafa Soliman, Independent Researcher, USA. E-mail: mostafasoliman.am@gmail.com*

[1] William E. Olson, Jr. (2016). The Deep, Dark Web. *The Nebraska Lawyer*, March/April at 24.

[2] *Id.*

[3] *Id.*

2790-1386/© 2023. Mostafa Soliman. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

using traditional search engines.[4] The Dark Net is a subset of the Deep Web and can only be accessed using specialized tools like Tor. It serves as an underground market on the Internet, and while its exact size is difficult to determine, it is estimated to be 400-500 times larger than the Surface Net.[5] To put it in perspective, the data stored on the 60 largest Deep Web sites is 40 times larger than the entire Surface Net.[6]

There are two types of Dark Net: Friend-to-Friend networks that are primarily used for file sharing through peer-to-peer connections, and privacy networks like Tor.[7] Accessing the Dark Net requires using Tor software to access sites with a ".onion" designation.[8] Tor's function is to keep users anonymous, and Bitcoin is commonly used as a method of payment.[9] The Dark Net is infamous for its illegal activities, including the sale of drugs, personal and financial information, counterfeit goods, pharmaceutical prescriptions, child pornography, and even the hiring of hit men.[10] In 2013, the FBI arrested Ross Ulbricht and shut down Silk Road, one of the largest marketplaces on the Dark Net.[11] It is estimated that Ulbricht made over $80 mn from Silk Road, which offered both legal and illegal goods and services.[12]

The Tor network was originally designed by the Naval Research Lab, which received 60% of its support from the State Department and Department of Defense.[13] These government agencies supported Tor as a means of secure communication between themselves and dissidents fighting oppressive regimes.[14] Private institutions also use Tor, such as The New York magazine, which operates a hidden Tor services site called Strongbox to allow whistleblowers to anonymously and securely communicate information with the magazine.[15]

2. The Relationship Between the Internet, Dark Web and Dark Net

The Federal Networking Council (FNC) provides a definition for the Internet as a global information system that is connected through a unique address space based on the Internet Protocol (IP).[16] The system supports communication using various IP-compatible protocols and provides high-level services. International Corporation Assigned Names and Numbers (ICANN) administers the address or name spaces to ensure the security, stability, and interoperability of the Internet.[17]

The World Wide Web (WWW) is an Internet-based system that allows individuals or companies to share information globally, except in regions where the free interchange of information is restricted.[18] Prior to the WWW, different systems with unique structures and indexes existed.[19] The development of browsers and search engines such as Google made the surface web, which is accessible to everyone, a reality.[20]

[4] *Id.*

[5] Sui, Daniel, James Caverlee. and Dakota, Rudesill. (2015). The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. October at 6.

[6] *Id.* Page 5.

[7] *Supra* Note 1 at 24.

[8] *Id.* Page 25.

[9] *Id.*

[10] *Id.*

[11] Jeffray, Calum. and Tobias, Feakin. (2015). Underground Web The Cybercrime Challenge. *Special, International Cyber Policy Centre*, Australian Strategic Policy Institute. p. 11.

[12] *Id.*

[13] *Supra* Note 1 at 25.

[14] *Id.*

[15] *Id.*

[16] Barry M. Leiner., Vinton G. Cerf., David D. Clark., Robert E. Kahn., Leonard Kleinrock., Daniel C. Lynch., Jon Postel., Larry G. Roberts. and Stephen Wolff. (n.d.). *Brief History of the Internet.* Accessed on September 19, 2016. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

[17] ICANN. (n.d.). Resources. *ICANN Website.* Accessed on September 19, 2016. https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf.

[18] PC Magazine. (n.d.). *Encyclopedia.* Accessed on September 19, 2016. http://www.pcmag.com/encyclopedia/term/54867/world-wide-web.

[19] *Supra* Note 1 at 23.

[20] *Id.*

The Internet consists of the Surface Web, Deep Web, and Dark Web. The Surface Web contains only 4% of the Internet's data, while the remaining 96% is located in the Deep Web.[21] Search engines cannot index the Deep Web.[22] For instance, a bank provides clients access to their accounts via the Surface Web, but the usernames and passwords are stored in the hidden Deep Web.[23]

The Dark Web is a part of the Deep Web and can only be accessed through Tor or Peer-to-Peer networks.[24] Another level of Net is the Darknet, which is part of the Dark Web.[25] The Deep Web is not indexed and cannot be reached by ordinary search engines.[26] Google has only indexed up to 16% of the Surface Web, whereas the Deep Web is nearly 400-500 times larger than the Surface Web. Thus, the three levels of the Internet are interconnected.[27]

3. Legal Framework

An international regulation specifically for the Dark Net does not currently exist for the international community. There are however existing international laws for cooperation in enforcing violations of national laws and trade conventions.[28] The criminalization of acts involving Dark Net usage depends on national laws that criminalize the use of hacking tools as a violation of computer crime laws, such as the Computer Fraud and Abuse Act in the USA.[29]

3.1. 2001 Budapest Convention on Cybercrime[30]

The Convention on Cybercrime aims to create a uniform legal framework for cybercrime and facilitate international cooperation in investigating and prosecuting such crimes.[31] Cybercrimes are defined as those committed using a computer as either a tool or a target.[32] The convention has been ratified or acceded to by 49 countries, including most members of the Council of Europe as well as non-members such as the United States.[33] Article 6 of the Convention criminalizes the sale, procurement, import, and distribution of code and other hacking tools.[34] Despite the existence of the convention, however, effective control over the Dark Net remains elusive.[35]

The growth and scope of crypto markets, which are online forums where goods and services are exchanged using digital encryption to conceal identities[36], present law enforcement agencies with significant challenges related to cybercrime and anonymity.[37] To address these issues, it is recommended that efforts be focused on three key areas.[38] The first is the development and deployment of new technologies, such as cloud computing, to effectively combat the rapidly growing Dark Net.[39] Second, there is a need to train and maintain skilled teams to leverage technology in the fight against cybercrime.[40] Finally, building international partnerships is

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Supra* Note 6.

[27] *Id.*

[28] *Id.* at 11

[29] *Id.*

[30] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[31] *Supra* note 6 at 11.

[32] Joseph, Aghatise E. (2006). *Cybercrime Definition.* June 28. Accessed on September 19, 2016. www.crime- research.org/articles/joseph06.

[33] Council of Europe, Chart of Signatures and Ratifications of Treaty 185 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=hnwADLWs

[34] *Supra* note 6 at 11.

[35] *Id.*

[36] Martin, James. (2014). *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drgus* at 2.

[37] *Supra* note 12 at 14.

[38] *Id.*

[39] *Id.*

[40] *Id.*

crucial given the lack of boundaries in cyberspace. By focusing on these areas, law enforcement agencies can enhance their ability to effectively combat cybercrime and maintain public safety.[41]

4. Conclusion

The Dark Web poses a significant challenge due to the evolution and complexity of information systems and the internet. With various layers of the internet, including the Surface Web, Deep Web, and Dark Web, only a small part of the internet is publicly accessible. The Deep Web and Dark Web remain hidden from ordinary search engines and are not easily accessible due to encryption and anonymity. This presents significant challenges to law enforcement agencies in their efforts to combat cybercrimes.

International cooperation is greatly needed to harmonize criminal laws and improve investigations in cybercrime matters. To continue combating cybercrimes effectively, law enforcement agencies must develop new technologies, maintain skilled teams, and build international partnerships.

References

Barry M. Leiner., Vinton G. Cerf., David D. Clark., Robert E. Kahn., Leonard Kleinrock., Daniel C. Lynch., Jon Postel., Larry G. Roberts. and Stephen Wolff. (n.d.). *Brief History of the Internet*. September 19, 2016. <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>.

ICANN. (n.d.). Resources. *ICANN Website.* September 19, 2016. <https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf>.

Jeffray, Calum. and Tobias Feakin. (2015). Underground Web The Cybercrime Challenge. Special. Australian Strategic Policy Institute.

Joseph, Aghatise E. (2006). *Cybercrime Definition*, June 28, 2006. Sept ember 19, 2016. <www.crime-research.org/articles/joseph06/>.

Martin, James. (2014). *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drgus.*

PC Magazine. (n.d.). *Encyclopedia*. September 19, 2016. <http://www.pcmag.com/encyclopedia/term/54867/world-wide-web>.

Sui, Daniel., James Caverlee. and Dakota Rudesill. (2015). The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. October.

William E. Olson, Jr. (2016). The Deep, Dark Web. *The Nebraska Lawyer,* March/April 2016.

[41] *Id.*

Cite this article as: Mostafa Soliman (2023). Layers of the Internet: The Challenge of the Dark Web and the Need for an International Legal Framework. *International Journal of Cryptocurrency Research*, 3(1), 74-77. doi: 10.51483/IJCCR.3.1.2023.74-77.